BPTrends ARTICLE

Managing Risks with an End-to-End Process View

Adopting a process-based approach to risk management

03/04/2014
Gail P. Evans

Overview

How does an organization create a sustainable process, where natural tensions exist between the players, so that:

- the end-to-end process fosters cross-functional cooperation
- objectives are achieved
- the critical risks are managed appropriately?

In his article "Operational risk: Lessons from non-financial organizations", Simon Ashby writes about adopting a process-based approach to risk management. "The key to the effective adoption of the process approach is comprehensiveness. Such an approach should not only look at the organization's frontline processes, but also all of its back-office and support processes (finance, HR, IT, etc.)" (Ashby, 2008, p. 413).

While he speaks of applying risk management processes at an enterprise level, one can also apply this principle to specific processes. By incorporating risk management into a process, it is possible to bring the front and back offices together to achieve business goals in a sustainable manner.

This Article examines the link between strategy, process and risk management and explains how one governance, risk and compliance framework in particular, developed by the nonprofit group OCEG[1], can be leveraged to ensure that critical business processes effectively support an organization's strategy.

Managing risk while enabling business

To manage risk thoughtfully using a process-based approach, one must consider the "comprehensiveness" of a process: Where does a process start and end? Are all of the right players involved?

It is not enough to simply include process participants who have a stake in the end-to-end outcomes to manage risk. To build on Ashby's advice, one should look to governance, risk and compliance (GRC) frameworks to ensure that sub-processes are sufficiently integrated to manage risk effectively and efficiently, increasing the likelihood of implementing smart and sustainable risk management that promotes, rather than inhibits, business.

Leveraging the OCEG Capability Model to Assess the Ability of an End-to-End Process to Optimize Risk and Reward

The GRC Capability Model was developed by OCEG, a non-profit think tank founded in 2002, in response to the significant dot.com and corporate failures that plagued the late 1990's and early 2000's. The OCEG Red Book, which is open source, sets forth elements that should result in sound governance, risk and compliance

[1] www.oceg.org

management to drive expected outcomes, including achieving business objectives, enhancing organizational culture and increasing stakeholder confidence (Scott R. Mitchell, 2012, p. 17). OCEG refers to this as "Principled Performance"™—defining GRC as "a capability that enables the organization to reliably achieve objectives while addressing uncertainty and acting with integrity" (Scott R. Mitchell, 2012, p. 19). Unlike COSO or ISO standards, the framework is flexible—not all elements must be adopted—and can be applied entity-wide or to a particular compliance program, such as anti-money laundering.

The OCEG Capability Model is made up of eight components, which are depicted in the graphic below.

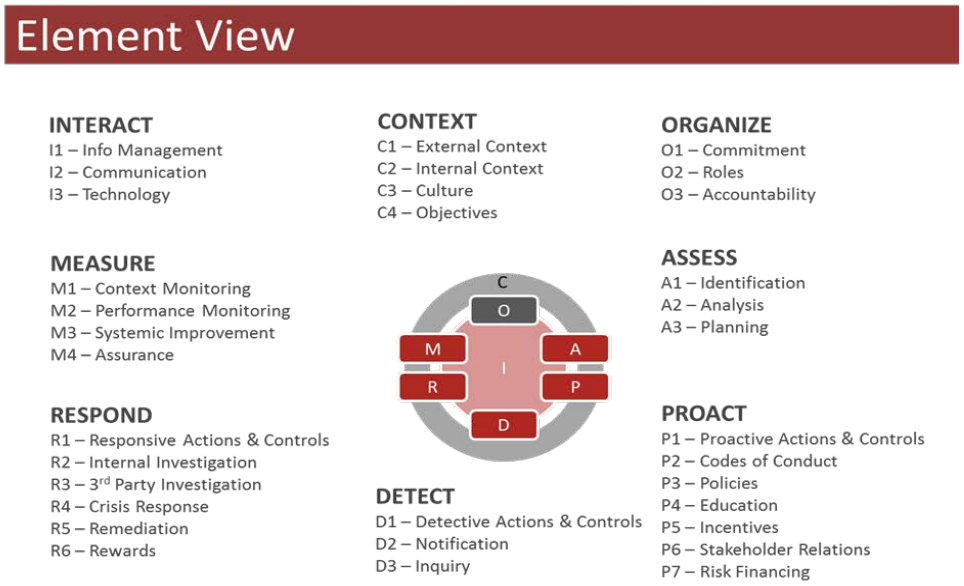

Figure 1 – OCEG Capability Model (Scott R. Mitchell, 2012, p. Intro 6)

According to the Red Book, the GRC Capability Model can be applied at both an enterprise-wide and organizational level and should generally be applied in the order listed:

"Components embody integrated Elements of a high performing GRC capability to support both universal and organizational objectives. They operate in a somewhat sequential manner; however, a user may begin to apply the Red Book at any of the Component points as a means of maturing existing capability. All components must operate continuously to realize a high-performing GRC." (Scott R. Mitchell, 2012, p. Intro 5)

In other words, at the outset, each of the eight components can only be appropriately derived if the preceding component has been clearly defined. Following

Choosing a GRC Model

Many enterprise risk management (ERM) frameworks exist that can provide some insights into risk management: COSO ERM and ISO 30001:2009 are two that are referred to most often. COSO ERM (Committee of Sponsoring Organizations of the Treadway Commission) was first issued in 2004 to give guidance to organizations to help design and implement internal controls and assessing their effectiveness. COSO ERM provides a way to evaluate ERM programs, rather than focusing on risk management activities (Deloach, 2012). Although it speaks to strategy, because of its genesis, COSO ERM tends to be associated more with compliance and the performance of internal controls than with the practical implementation of risk management. ISO 30001:2009, on the other hand, provides principles and generic guidance for risk management.

A third overarching framework exists which incorporates elements of COSO ERM and ISO 300001, along with other standards—such as ITIL[1] and ISO 9000—and regulatory requirements, to c777reate an environment where business risks are measured and relevant information is communicated and leveraged by management to make sound business decisions. This framework, the OCEG GRC Capability Model—which is outlined in what is referred to as the Red Book—provides more in-depth context on culture and internal and external constraints than COSO ERM or ISO 30001, combining various good practices to optimize a company's performance.

the same premise that process improvement activities should not be undertaken if they do not support business strategy, GRC activities should first be driven by an entity's business.

***Context**:* Which customer needs is the organization trying to address? What is the organization's strategy to address those needs and how do its vision and mission align to it? Within which constraints must it or is it willing to work (i.e. regulatory versus voluntary boundaries)? *Context* is also defined by corporate culture—setting a clear tone at the top for expected behaviors and desired results. Based on these elements, what objectives does the organization set for itself? Once these elements are defined, the organization can define its risk appetite—to how much risk is the organization is willing to expose itself in pursuit of opportunity to ensure that objectives can be reasonably achieved?

Context in turn drives an entity's ability to ***Organize*** itself. Once it determines the direction in which it wants to head, the organization can define the scope of its GRC capabilities to manage getting there. Critical success factors to the *Organize* element are: (1) a GRC charter aligned to the organization's objectives, (2) support for the program from the board and key senior leadership and (3) defining and describing the GRC framework to demonstrate that it enables the governance, management and assurance that business goals will be met, while managing risk and compliance (Scott R. Mitchell, 2012, p. 20). Similarly, a business process should be aligned with the organization's objectives, enjoy the sponsorship and buy-in of senior and executive management and be communicated in such a way that process participants understand the value the process brings to managing business risk while achieving corporate goals.

Once the GRC framework is organized, the next step in the Capability Model is to continuously ***Assess*** threats and opportunities. This involves weighing the effects of risk and reward to the organization to determine whether the inherent levels of both remain within the bounds of the organization's risk appetite (as defined in the *Context* component). Control activities are then developed to either prevent the organization from going outside of the defined boundaries (i.e. ***Proact***) or *Detect* when those boundaries have been exceeded after the fact. The same can be said of any process, where threats to achieving objectives must be assessed and preventive or detective controls put in place to manage those risks effectively and efficiently, without over- or under-controlling them. Systems must then be put in place to ***Respond***, rewarding desirable conduct and discouraging non-compliance with the established framework. In the case of process compliance, this can include incentives for applying appropriate behaviors which are critical to achieving objectives.

Once defined and operational, the GRC framework must be ***Measured*** and adapted as appropriate. Likewise for any process, in order to ensure that it is sustainable and continues to address an organization's business goals, process performance must be monitored and measured. Finally, a framework must be established to allow GRC elements to ***Interact***, sharing the information gathered from the preceding elements so that corrective actions can be taken and improvements made.

The following table summarizes the eight components of the GRC Capability Model at a high level, based on OCEG's Red Book 2.1, and provides some examples of elements that can be considered to support each component. When combined properly, these elements should enable sound business decisions, optimizing risk and

opportunity. At the same time, as the Red Book notes, provided that some form of framework is already in place, an organization can work on certain elements, enhancing weaker links in the framework to strengthen it overall.

OCEC GRC Components	OCEG GRC Framework Elements
Context *Understand the current culture and business context so that the organization can address and proactively influence conditions to support objectives*	1. External context (environment, stakeholder needs) 2. Internal context (strategy, organizational structure, resources) 3. Culture (ethics, risk, governance, engagement) 4. Objectives (mission, vision, objectives, values)
Organize *Organize and oversee an integrated capability that enables the organization to reliably achieve objectives while addressing uncertainly*	1. Define goals of GRC system to support business objectives; obtain commitment to the capability 2. Assign management responsibilities, authority and accountability 3. Define approach to embed, integrate and align GRC capability with business and establish accountability
Assess *Identify opportunities, threats and requirements, assess the level of risk, reward and conformance; and align an approach to reliability achieve objectives while addressing uncertainty and acting with integrity*	1. Identify opportunities, threats and requirements 2. Assess level of risk and reward 3. Align approach to achieve objectives while addressing uncertainty and acting with integrity
Proact *Proactively incent desirable conditions and events; and prevent undesirable conditions and events with management actions and controls*	1. Promote desirable events/prevent undesirable events 2. Codes of conduct for all levels and extended enterprise 3. Policies aligned with opportunities, threats and requirements 4. Educate all levels about expected conduct, increase skills needed to address threats opportunities and requirements 5. Incentivize desirable conduct 6. Stakeholder relations to shape expectations and influence perspectives 7. Risk financing to reduce or remove impact of threats

Detect *Detect ongoing progress toward objectives as well as actual and potential undesirable conditions and events using management actions and controls*	1. Establish detective controls 2. Capture results and notify stakeholders of undesirable conditions 3. Gather information, self-assess and report on progress toward objectives
Respond *Respond to desirable conditions and events with rewards; and correct undesirable conditions and events to that the organization recovers from and resolves each immediate issue and improves future performance*	1. Reward desirable conduct, discipline undesirable conduct 2. Review and investigate misconduct 3. Manage and respond to external inquiries and investigations 4. Plan for and respond to crisis issues, business disruptions 5. Resolve substantiated issues 6. Recognize and incentivize positive contributors
Measure *Monitor, measure and modify the capability on a periodic and ongoing basis to ensure that management actions and controls reliably achieve objectives while addressing uncertainly and acting with integrity*	1. Monitor internal and external context 2. Monitor and evaluate design, performance; analyze and report results 3. Improve systematically 4. Assure reliability, effectiveness and efficiency of overall model
Interact *Enable capability with technology and manage information so that it efficiently and accurately flows up, down and across the organization, extended enterprise, and to appropriate stakeholders*	1. Develop framework to manage information 2. Develop reporting and communications plan 3. Assess technology needs and gaps to manage GRC

Table 1 – OCEG GRC Elements (Scott R. Mitchell, 2012, p. Intro 5)

Applying the Capability Model to Assess Strategy Execution Risks

Any organization can follow the principles of the OCEG's Capability Model to ensure processes are sustainable and enable sound business decisions that optimize risk and opportunity. Such analysis can be performed at any time for any process. An ideal time to perform it, however, is when an organization's strategy changes, or there have been significant changes to the external and/or internal context within which the organization operates. Applying the following approach at that time ensures that the front and back offices remain aligned end-to-end so that they can execute the new strategy, making it achievable and sustainable. The following steps can be used to accomplish this:

1. Identify and document the organization's industry risks

a. Risk—Determine and document risk categories (such as regulatory, legal, operational, financial).

b. Risk Events—What could go wrong if processes are not functioning as designed? Consider potential missteps by the organization, suppliers or customers and potential impacts to all parties in the value chain.

c. Potential Impacts—Document what might happen to the organization and its stakeholders if the risk event were to occur.

2. Map industry risks to the processes that are impacted by the change

a. At what points is the process capable of impacting the objectives of the corporate strategy?

b. Which elements of the process are critical to optimize risk and reward (such as risk assessments and go/no-go decision points, process monitoring)?

c. Which elements are critical to the sustainability of the process (such as aligned objectives across functions, process training)?

3. Based on impacts identified above, select key process(es) to be analyzed that will be impacted by change in strategy

a. Determine process scope and identify end-to-end participants.

b. Consider the suppliers and customers (internal and external) using a scoping diagram. (My preferred scoping methodology is BPTrends IGOE Diagram,[2] which identifies inputs, guides, enablers and outputs, taking regulations and corporate policies and procedures explicitly into account.)

4. Assess the process' strengths and weaknesses against the Capability Model

a. Refer to the Red Book determine which of the framework's many factors are most relevant to the process in question. It's not necessary to map to all factors, only those that will make or break success.

b. For each of the eight Red Book GRC components, document the strengths and weaknesses that contribute to the process' success or could result in breakdowns.

5. Address any critical weaknesses that present execution risk to the strategy

a. Agree on pain points of the current process which would hinder achieving the new strategy or cause inefficiencies that are otherwise worth addressing.

[2] http://www.bptrends.com/publicationfiles/advisor20121009.pdf

b. Build a road map for process improvements to manage execution risk and increase efficiencies.

If your organization is not at a level of maturity where each critical process has been linked to its role in the strategy, it will be challenging to weave these elements together. In order to build a seamless and sustainable approach to managing risk within a process, you should first review your critical processes to ensure that they actually contribute to your strategy.

Applying Risk Management Frameworks to Processes in General

In his article, Ashby writes, "Adopting a process-based approach [to risk management] undoubtedly incurs considerable upfront costs and demands the careful mapping of all an organization's processes and sub-processes. However, the benefits can be considerable and may even extend beyond the operational risk manager's traditional habitat of loss identification and reduction to include the exploitation of potential efficiency gains via the streamlining of overly complex and time-consuming processes" (Ashby, 2008, p. 413).

A few elements can be combined with the foundations of good business process management to manage risk in general:

1. Tie the process to the organization's strategy

   a. The end-to-end process, including back-office functions, must support the strategy.

   b. When strategies are modified to address new opportunities, risks must be reassessed. Supporting processes must be assessed and resources realigned to balance risk and opportunity.

   c. Link objectives of process participants to the end result of the process so that everyone is working with the same goal in mind.

2. Do not make risk management complicated. Build it into existing operational processes so it becomes second nature.

   a. Automate workflows to facilitate execution.

   b. Reward systems should deter undesirable behaviors and encourage the right ones.

3. Knowledge

   a. Educate employees and customers about relevant risks. Employees must be able to articulate risks and defend the company's standards with conviction.

   b. Ensure that all participants—including customers—have appropriate level of knowledge of the end-to-end process and how elements within a process help mitigate those risks.

   c. If your business has high barriers to entry, do not put off the discussion—if a prospect is not prepared to comply with your standards, better to know that

up front and save scarce resources. Discussing potential issues early on gives them time to think about and address them, managing the customer's expectations of time-to-market.

d. Share information at the right levels and right time to inform sound business decisions.

4. Monitoring and Reevaluation

a. Monitor and reevaluate the process periodically to ensure efficiency and effectiveness.

b. Monitor and reevaluate customer risk profiles periodically to determine if controls can be dialed back or must be increased.

c. Automate monitoring tools so results can be easily measured.

d. Select the right measures to track progress towards objectives.

Thinking more holistically about governance, risk and compliance when examining key processes should strengthen an organization's ability to balance risk and opportunity as the business evolves in response to internal and external factors, while remaining responsive to customer needs.

References

Ashby, S. (2008). Operational Risk, Lesson from non-financial organizations". *Journal of Risk Management in Financial Institutions, 1*, 406-415.

Deloach, J. (2012, June 25). *COSO, ISO 31000 or Another ERM Framework?* Retrieved July 2, 2012, from Corporate Compliance Insights: www.corporatecomplianceinsights.com/coso-iso-31000-or-another-erm-framwork?

Scott R. Mitchell, C. S. (2012). *OCEG Red Book GRC Capability Mode 2.1.* Open Compliance & Ethics Group.

Author

Gail Evans has 25 years' experience in compliance and internal controls, having served as an international corporate tax consultant and managed regional internal audit departments, amongst other roles. In the past few years, she has been pursuing her interest in business process management, looking for ways for her colleagues to work more efficiently while still managing risk effectively. As a vice president at MasterCard, she aligns process and strategy for Global Sales Effectiveness.

Gail holds a B.A. in English Literature and certificate in Accounting from the University of Virginia. She also holds a certification in Business Process Management from Vlerick Business School in Belgium.